11. Assignment

Computer Security Summer 2021

Deadline: July. 8th 2021, 12:00

Remarks

(a) Upload one and only one PDF-file.

(b) Groups of 2-3 persons are allowed.

(c) You can use our Latex-template.

(d) Your solution should be properly anonymized (no names, no contact information).

(e) **Topics of this assignment:** You should be familiar with the topics of *03_policies_5* and *03_policies_6*.

Exercise 1 Real world access control matrix *3 points*

Consider the standard Unix permissions in a Linux or BSD file system with users, groups, files and the access rights *read*, *write* and *execute*.

(a) Explain how to model this system using the access control matrix model, i.e. define rights and explain which roles take subjects and objects. In particular, how can you model group-relationships and rights?

(b) Now consider the following example (left) taken from a Linux file system and a corresponding `groups` file (right).

```
drwxr-xr-x  alice users .
drwxr-xr-x  alice users ..
-rwxr--r--  alice f     A
-rwxrw----  alice bfct  B
-rwxr-----  frank c     C
-rw-r-----  bob   at    D
-r-xr-x---  tim   ct    E
-r-----r--  carl  c     F
```

```
f:*:1000:frank
bfct:*:1001:bob,frank,carl,tim
c:*:1002:carl
ct:*:1003:carl,tim
at:*:1004:alice,tim
other:*:99:
```

Model the permissions indicated by this file listing in the *access control matrix model* using your approach.

Exercise 2 HRU Model (Access Control Matrix) *3 points*

In class we modeled the primitive actions `create subject` s, `destroy subject` s and `enter` r `into` s, o using preconditions and postconditions. Model the remaining primitive actions

(a) `create object` o,

(b) `destroy object` o, and

(c) `delete` r `from` s, o

in the same way.

2

a) Operation - create object o

Precondition - $o \notin O$

Postcondition - $S' = S$

- $O' = O \cup \{o\}$
- $\forall s' \in S' : M'(s', o) = \phi$
- $\forall s \in S \, \forall o_2 \in O : M'(s, o_2) = M(s, o_2)$

Operation - destroy object o

Precondition - $o \in O$

Postcondition - $S' = S$

- $O' = O \setminus \{o\}$
- $\forall s' \in S' : M'(s', o) = \phi$
- $\forall s' \in S' \, \forall o' \in O' : M'(s', o') = M(s, o)$

Operation - delete r from s, o

Precondition - $s \in S$, $o \in O$

Postcondition - $S' = S$, $O' = O$

- $M'(s, o) = M(s, o) \setminus \{r\}$
- $(\forall s_2, o_2 \in S \times O \setminus \{s, o\})$: $M'(s_2, o_2) = M(s_2, o_2)$

We used this source to compare our results:

https://www.cs.purdue.edu/homes/clifton/cs526/HRU.pdf

①